Exhibit A

EXPERT REPORT
SERGE EGELMAN, PH.D.

CONTENTS

1. QUALIFICATIONS

My name is Serge Egelman, and I direct the Usable Security & Privacy research group at the International Computer Science Institute (ICSI), which is a research institute affiliated with the University of California, Berkeley, where I also hold an appointment within the Department of Electrical Engineering and Computer Sciences (EECS). My laboratory performs research at the intersection of online privacy, security, and human factors ("human-computer interaction" or HCI). Specifically, we apply social sciences research methods to understand how people make decisions about their online privacy and security. This involves conducting surveys, interviews, and controlled experiments, which are regularly published in peer-reviewed journals and conference proceedings.

I received my Ph.D. from Carnegie Mellon University's School of Computer Science and have been conducting research in this area for almost 20 years now. I have over 100 peer-reviewed research publications, many of which use research methods like surveying, interviewing, and performing behavioral experiments. My research has been cited over 10,000 times, including in multiple judicial opinions and regulatory enforcement actions. My h-index, a commonly used metric for academic impact, is 47.[1]

In addition to my academic research performing surveys, interviews, and other human subjects research, I also have over ten years of experience analyzing the privacy and security behaviors of mobile apps. Research by my laboratory to develop tools to analyze the privacy behaviors of mobile apps has been commercialized via AppCensus, Inc., a company I co-founded and serve as CTO for. AppCensus performs analysis of mobile apps for privacy compliance purposes, assisting both enterprise software developers and compliance professionals, as well as regulators, law firms, and watchdog groups. The underlying research has received multiple awards, including the top privacy research awards from the Spanish and French data protection agencies, and data from the tools has been used by multiple state attorneys general and the FTC. Through this research, I have become an expert on mobile privacy and the app ecosystem (and have testified before Congress on these issues).

[1] https://en.wikipedia.org/wiki/H-index

2. BACKGROUND

This case stems from the disclosures used by The Weather Channel's (TWC) mobile app in communicating if and how consumers' location data will be used. As a preliminary matter, I examined several prior versions of the iOS and Android apps. On iOS, when runtime permission requests are shown to users, app developers can optionally include text that explains the rationale for the request. Both the Hanssens and Snow reports purport to examine the effects of this text through a survey (Hanssens) and analysis of log data (Snow).

Both reports focus on the disclosure shown in the center of Figure 1, which tells users that if allowed, "[y]ou'll get personalized local weather data, alerts and forecasts." This disclosure was in use from February through September 2017, though only when the app requested *background* location access; this language was used again from November 2018 through January 2019, when requesting *either* background or foreground access. In January 2019, it was updated to state, "[w]e use and share your location data as described in our privacy policy, including to provide you with personalized local weather data, alerts, and geographically relevant advertising." Previously, the disclosure stated, "[w]e use your location to provide you with accurate weather data and forecasts." This specific statement was in use from at least 2014 through November 2018, when it was changed—albeit briefly—to the one examined in the Hanssens and Snow reports (i.e., the disclosure examined by both reports appeared to only exist for a few months, of the app's 5+ years of existence).

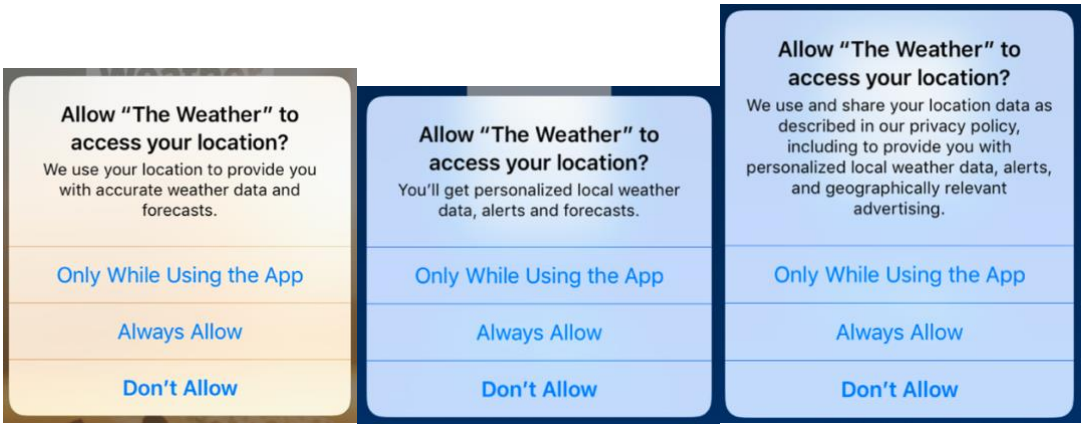

Figure 1: iOS location disclosures shown to users prior to November 2018 (left), November 2018 through January 2019 (center), and after January 2019 (right).

Beyond the disclosures, additional data was provided for drafting the Snow report, a subset of which was shared with me. This data purportedly came from Localytics, one of TWC's third-party location data recipients. The data purportedly contains communications sent by the TWC app from consumers' mobile devices, and contains information about the device, unique identifiers to identify the user, as well as information about that user's physical location. Consider the following example data transmitted in Figure 2.

Figure 2: Data transmitted to Localytics from the TWC app.

Based on my knowledge of the mobile app ecosystem and how data is transmitted between mobile apps and remote servers, this data set appears to contain the following information:

- Unique identifiers ("app") corresponding to the app (i.e., the data is identified as having come from the TWC app)
- The version of the app that sent the data ("app_vers")
- The time that the data was sent or receive ("at")
- The mobile carrier to which the user subscribes ("carrier")
- The country in which the transmitting phone is located ("country")
- The state or region in which the transmitting phone is located ("region")
- Identifiers that uniquely identify the user ("userId," "uuid," and "user_uuid") and/or device ("device_uuid")
- Specific events that occur while the user is using the app ("name")
- The phone's operating system and version ("platform" and "os_ver")
- The phone's make and model ("model")
- The type of data connection ("data_conn")
- The device's timezone ("device_timezone")

With this data, anyone can identify how many unique users were using TWC's app in a specified state or region at any given time. For example, this data appears to readily show how many users were located in a given state on a given day. The data includes the version of the TWC app used and the date and time of use. The version of the TWC app that was first used by any given user correlates to one of the three permission prompts used over the relevant time period. Based on my experience and expertise, I am confident that these identifiers are linkable to other persistent identifiers collected previously (and/or from other sources) and that user profiles can be created that identify individuals' physical locations over time, their routines, relations, interactions, and their preferences and interests based on the other websites and mobile apps that they use. TWC maintains geolocation data from users. This has been produced for one of the identifiers associated with the device of one of the named Plaintiffs which includes a lengthy history—dating back to 2016—of the locations where geolocation data—with latitude and longitude to the fifth decimal place—was collected. See*, e.g.,* TWC_HART_000010956.

3. Comments on Hanssens Report

The Hanssens report features a survey in which participants were shown text that was briefly used by TWC in the app: "you'll get personalized local weather data, alerts, and forecasts." Disclosures in use during the majority of the app's existence were not examined, and therefore this survey's results cannot be generalized to those other disclosures. Worse, survey results are confounded because responses were likely heavily impacted by priming: participants were asked specifically about ads starting in the second question of the survey (the first question was used for subterfuge), and then throughout. Thus, this survey suffers both from threats to internal validity (i.e., the data does not support the conclusions) and external validity (i.e., it cannot be generalized to a broader population), and therefore should be rejected.

3.1 Threats to Internal Validity

The disclosures shown in the survey were only in use by the TWC app for a fraction of the class period. Unlike other disclosures used by the app (e.g., "we use your location to provide you with accurate weather data and forecasts"), the disclosure chosen for the survey specifically used the word "personalization." The survey's early focus on advertising may have primed respondents. The survey never asked participants what they believed the statement meant without first priming them to think about advertising. A neutral approach would have been to ask respondents how they expected their data to be used based on the disclosure, and then ask them to choose from several multiple-choice options (of which "advertising" is one of many choices) or respond with a free-form text box. As a result, without priming, we have no idea whether or not respondents would have associated the specific disclosure with advertising. This issue of priming is a serious confounding factor that calls the internal validity of the survey into question (i.e., the survey design cannot support the conclusions in the report).

Another threat to internal validity is the timing of the two surveys: a second "robustness" survey was conducted to compare results from the first survey to identical disclosures in a fictitious app. Hanssens performed two separate surveys, using two separate samples, conducted during two different time periods. As a result, one cannot directly compare the results of one survey with the other. A more scientifically valid design would be to conduct a single survey, in which app branding

is treated as a dependent variable (i.e., TWC vs. a fictitious app), to then examine whether responses (i.e., independent variables) appreciably change as a function of that branding. In doing this experiment, one would need to recruit a single sample of participants who would each be randomly exposed to one of the treatments. However, that was not what was done, and as a result, the time gap and varying samples represent confounding factors that further diminish the internal validity of the survey.

3.2 Threats to External Validity

In addition to the internal validity issues I have outlined, the survey also suffers from external validity issues (i.e., it cannot be generalized to the broader population). First, it is not clear that the sample surveyed are representative of members of the impacted class. Respondents were screened out based on their self-reported memory of having previously installed the TWC app. However, this is obviously subject to recall bias: many respondents may not remember having installed the TWC app nor whether they granted it access to location data.

Worse, people who can remember having installed the TWC app are not necessarily the correct population from which to sample. In identifying a sample to recruit for a survey, it is important that the sample be "similarly situated" to the target population. The target population is not all users who can recall both using the TWC app and granting it access to their location data, but instead should be TWC app users who are encountering the app's privacy disclosures for the first time and must use them to make decisions about their privacy. Existing app users have already made this decision and also may have heard information in the news about TWC's privacy practices. That is, Hanssens' sample of survey respondents are not similarly situated to those encountering the app for the first time before 2019. Because existing TWC users are likely tainted (i.e., they have already encountered TWC's disclosures and may have prior opinions about them), a proxy sample should have been used (i.e., survey respondents who have not already been exposed to the specific disclosures nor popular media reporting of TWC's alleged misrepresentations).

Another issue with generalizability is due to the timing of the survey. As I noted previously, the research question that the survey *should* have answered is whether a reasonable person at the time that they encountered the disclosures would understand that location data would be sold to advertisers. However, the survey was performed in 2022, and not at the time that consumers encountered the disclosures for the first time. It is well documented that consumer privacy concerns have been increasing over the past 50 years, moreso very recently. In particular, the collection of location data has been in the news fairly regularly over the last several years, and as a result, consumers surveyed today would be more likely to be suspicious that their information may be used for secondary purposes than if asked 3–4 years ago. As a result, this survey tells us very little about what the average consumer would understand about the disclosures at the time that they would have first encountered them.

3.3 Other Miscellaneous Issues

Separately, Hanssens claims that the use of data for advertising purposes is mentioned within the app's settings, but fails to note that this text was only added in mid-2018, and requires navigating through several layers of menus to see it. Whereas the "purpose string"—the text shown

within the permission request that is the primary focus of the survey—is shown to users whenever the app requests access to location data for the first time. That is, every consumer who agrees to allow access to their location data will see the purpose string, whereas only those using specific versions of the app and who bothered to navigate through layers of settings may see the additional disclosure.

The survey mentions a low margin of error, but this is a red herring. "Margin of error" is a measure of external validity: assuming a survey that is (1) free of bias and other confounding factors and (2) randomly sampled from a representative population, margin of error shows how likely the results are to translate to that broader population. However, both of these assumptions were violated by this survey—it was not free of bias and/or confounding factors and it is not clear that those sampled were representative of the target population—and therefore the margin of error cannot be calculated or interpreted.

Regarding footnotes 54 and 60, as an author of the paper cited, I can state that our goal was to examine consumers' expectations about what an app would do with their data based on whether or not they paid for it; we did not show participants any sort of disclosures, and contrary to the claims in the report, we did not ask participants about location data. What we did in our study was very different than showing someone a disclosure and then asking them what they expect will happen *based on* that disclosure; we examined consumer perceptions in the *absence* of disclosures. The real research question relevant to this survey should be what participants expect to happen *after seeing a disclosure* (that says data will only be used for a limited purpose), not based on whether or not they paid for the app.

4. Comments on Snow Report

From Snow's report, it is unclear whether he correctly identified how many users actually saw the updated version of the permissions prompt. In iOS, users were shown the permissions screen in Figure 2 the first time that they ran the app, and then could only revisit this decision through a system-wide settings panel. Snow's report is unclear as to whether existing TWC app users would have seen the updated disclosures in Figures 3 and 4 upon updating the app, or if only new users would have seen them. A related issue is that Snow appears to perform his analysis based on all active users' settings (or uninstalls) on a given day, and not based on what disclosures users actually saw.

As I noted earlier, the permission prompt depicted in Figure 2 of the Snow report was only in use by versions of the app released between approximately November 2018 and January 2019, whereas during the remainder of the class period—and the app's existence—different prompts with different text were shown to users. In his report, Snow erroneously claims that the featured prompt and text were in use since February 2017.

Dated: May 20, 2022 */s/Serge Egelman*

5. CURRICULUM VITAE

SergeEgelman

contact
2150 Shattuck Avenue
Suite 1100
Berkeley, CA 94704
USA

+1 (434) 227 1337

egelman@cs.berkeley.edu

education

2009	**PhD** in Computation, Organizations, and Society School of Computer Science	Carnegie Mellon University
2004	**BS** in Computer Engineering School of Engineering and Applied Science	University of Virginia

experience

2019–Now	**AppCensus, Inc.** CTO / Co-Founder	San Francisco, CA
2016–Now	**International Computer Science Institute** Research Director, Usable Security & Privacy Group	Berkeley, California
2013–2016	**International Computer Science Institute** Senior Researcher, Networking and Security Group	Berkeley, California
2011–Now	**University of California, Berkeley** Research Scientist, Electrical Engineering and Computer Sciences	Berkeley, California
2010–2011	**National Institute of Standards and Technology** Research Scientist, Visualization and Usability Group	Gaithersburg, Maryland
2009-2010	**Brown University** Postdoctoral Researcher, Computer Science Department	Providence, Rhode Island
2008	**Microsoft Research** Research Intern, Security and Privacy Group	Redmond, Washington
2008	**Microsoft Research** Research Intern, VIBE Group	Redmond, Washington
2006	**PARC** Research Intern, Computer Science Laboratory	Palo Alto, California

publications

refereed journal publications

Data Collection Practices of Mobile Applications Played by Preschool-Aged Children
Zhao, F., Egelman, S., Weeks, H. M., Kaciroti, N., Miller, A. L., and Radesky, J. S. JAMA Pediatrics *174.12 (Dec. 2020).*

Nudge Me Right: Personalizing Online Security Nudges to People's Decision-Making Styles
Peer, E., Egelman, S., Harbach, M., Malkin, N., Mathur, A., and Frik, A. Computers in Human Behavior *109 (Aug. 2020).*

Disaster Privacy/Privacy Disaster
Sanfilippo, M. R., Shvartzshnaider, Y., Reyes, I., Nissenbaum, H., and Egelman, S. Journal of the Association for Information Science and Technology *(Mar. 2020).*

Can You Pay For Privacy? Consumer Expectations and the Behavior of Free and Paid Apps
Bamberger, K. A., Egelman, S., Han, C., Elazari, A., and Reyes, I. Berkeley Technology Law Journal *35 (2020).*

The Price is (Not) Right: Comparing Privacy in Free and Paid Apps
Han, C., Reyes, I., Feal, Á., Reardon, J., Wijesekera, P., Vallina-Rodriguez, N., Elazari, A., Bamberger, K. A., and Egelman, S. Proceedings on Privacy Enhancing Technologies (PoPETS) *3 (2020).*

Investigating Users' Preferences and Expectations for Always-Listening Voice Assistants
Tabassum, M., Kosiński, T., Frik, A., Malkin, N., Wijesekera, P., Egelman, S., and Lipford, H. R. Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technoligies (IMWUT) *3.4 (Dec. 2019). Association for Computing Machinery.*

Privacy Attitudes of Smart Speaker Users
Malkin, N., Deatrick, J., Tong, A., Wijesekera, P., Wagner, D., and Egelman, S. Proceedings on Privacy Enhancing Technologies *2019.4 (2019).*

"Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale
Reyes, I., Wijesekera, P., Reardon, J., On, A. E. B., Razaghpanah, A., Vallina-Rodriguez, N., and Egelman, S. Proceedings on Privacy Enhancing Technologies *2018.3 (2018) pp. 63–83.* **Caspar Bowden PET Award**

A Usability Evaluation of Tor Launcher
Lee, L., Fifield, D., Malkin, N., Iyer, G., Egelman, S., and Wagner, D. Proceedings on Privacy Enhancing Technologies *2017.3 (2017) pp. 87–106.*

The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study
Tsai, J., Egelman, S., Cranor, L., and Acquisti, A. Information Systems Research *22.2 (2011) pp. 254–268.* **AIS Best Publication of 2011 Award / INFORMS Best Published Paper Award (2012)**

P3P Deployment on Websites
Cranor, L. F., Egelman, S., Sheng, S., McDonald, A. M., and Chowdhury, A. Electronic Commerce Research and Applications *7.3 (2008) pp. 274–293.*

The Real ID Act: Fixing Identity Documents with Duct Tape
Egelman, S., and Cranor, L. F. I/S: A Journal of Law and Policy for the Information Society *2.1 (2006) pp. 149–183.*

refereed conference publications

"You've Got Your Nice List of Bugs, Now What?" Vulnerability Discovery and Management Processes in the Wild
Alomar, N., Wijesekera, P., Qiu, E., and Egelman, S. Proceedings of the Sixteenth Symposium on Usable Privacy and Security *(SOUPS 2020), 2020.*

Actions Speak Louder than Words: Entity-Sensitive Privacy Policy and Data Flow Analysis with PoliCheck
Andow, B., Mahmud, S. Y., Whitaker, J., Enck, W., Reaves, B., Singh, K., and Egelman, S. 29th USENIX Security Symposium *(USENIX Security '20), 2020, Boston, MA.*

Don't Accept Candies from Strangers: An Analysis of Third-Party Mobile SDKs
Feal, Á., Gamba, J., Tapiador, J., Wijesekera, P., Reardon, J., Egelman, S., and Vallina-Rodriguez, N. International Conference on Computers, Privacy and Data Protection *(CPDP '20), 2020.*

A Qualitative Model of Older Adults' Contextual Decision-Making About Information Sharing
Frik, A., Bernd, J., Alomar, N., and Egelman, S. Workshop on the Economics of Information Security *(WEIS '20), 2020.*

Empirical Measurement of Systemic 2FA Usability
Reynolds, J., Samarin, N., Barnes, J., Judd, T., Mason, J., Bailey, M., and Egelman, S. Proceedings of the 29th USENIX Security Symposium *(USENIX Security '20), 2020.*

A Promise Is A Promise: The Effect of Commitment Devices on Computer Security Intentions
Frik, A., Malkin, N., Harbach, M., Peer, E., and Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '19), 2019.*

Privacy and Security Threat Models and Mitigation Strategies of Older Adults
Frik, A., Nurgalieva, L., Bernd, J., Lee, J. S., Schaub, F., and Egelman, S. Proceedings of the 15th Symposium on Usable Privacy and Security *(SOUPS '19), 2019, Berkeley, CA, USA.*

Information Design in An Aged Care Context
Nurgalieva, L., Frik, A., Ceschel, F., Egelman, S., and Marchese, M. Proceedings of the 13th International Conference on Pervasive Computing Technologies for Healthcare *(PervasiveHealth '19), 2019, New York, NY, USA.*

50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System
Reardon, J., Feal, A., Wijesekera, P., On, A. E. B., Vallina-Rodriguez, N., and Egelman, S. Proceedings of the 24th USENIX Security Symposium *(USENIX Security '19), 2019, Berkeley, CA, USA.* **USENIX Security Distinguished Paper Award / Emilio Aced Personal Data Protection Research Award**

An Experience Sampling Study of User Reactions to Browser Warnings in the Field
Reeder, R. W., Felt, A. P., Consolvo, S., Malkin, N., Thompson, C., and Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '18), 2018.*

Contextualizing Privacy Decisions for Better Prediction (and Protection)
Wijesekera, P., Reardon, J., Reyes, I., Tsai, L., Chen, J.-W., Good, N., Wagner, D., Beznosov, K., and Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '18), 2018.* **SIGCHI Honorable Mention Award**

Let's go in for a closer look: Observing passwords in their natural habitat
Pearman, S., Thomas, J., Naeini, P. E., Habib, H., Bauer, L., Christin, N., Cranor, L. F., Egelman, S., and Forget, A. Proc. of the ACM SIGSAC Conference on Computer & Communications Security *(CCS '17), 2017, New York, NY, USA.*

Turtle Guard: Helping Android Users Apply Contextual Privacy Preferences
Tsai, L., Wijesekera, P., Reardon, J., Reyes, I., Egelman, S., Wagner, D., Good, N., and Chen, J.-W. Proceedings of the 13th Symposium on Usable Privacy and Security *(SOUPS '17), 2017.*

The Feasibility of Dynamically Granted Permissions:
Aligning Mobile Privacy with User Preferences
Wijesekera, P., Baokar, A., Tsai, L., Reardon, J., Egelman, S., Wagner, D., and Beznosov, K. Proceedings of the 2017 IEEE Symposium on Security and Privacy *(Oakland '17), 2017.*

Do or Do Not, There Is No Try: User Engagement May Not Improve Security Outcomes
Forget, A., Pearman, S., Thomas, J., Acquisti, A., Christin, N., Cranor, L. F., Egelman, S., Harbach, M., and Telang, R. Proc. of the 12th Symposium on Usable Privacy and Security *(SOUPS '16), 2016.*

Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS)
Egelman, S., Harbach, M., and Peer, E. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '16), 2016.* **SIGCHI Honorable Mention Award**

The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens
Harbach, M., Luca, A. D., and Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '16), 2016.* **SIGCHI Honorable Mention Award**

Keep on Lockin' in the Free World: A Transnational Comparison of Smartphone Locking
Harbach, M., Luca, A. D., Malkin, N., and Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '16), 2016.* **SIGCHI Honorable Mention Award**

The Teaching Privacy Curriculum
Egelman, S., Bernd, J., Friedland, G., and Garcia, D. Proceedings of the 47th ACM technical symposium on Computer Science Education *(SIGCSE '16), 2016.*

Android Permissions Remystified: A Field Study on Contextual Integrity
Wijesekera, P., Baokar, A., Hosseini, A., Egelman, S., Wagner, D., and Beznosov, K. 24th USENIX Security Symposium *(USENIX Security 15), 2015, Washington, D.C.*

Is This Thing On? Communicating Privacy on Ubiquitous Sensing Platforms
Egelman, S., Kannavara, R., and Chow, R. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '15), 2015, New York, NY, USA.*

Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS)
Egelman, S., and Peer, E. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '15), 2015, New York, NY, USA.* **SIGCHI Honorable Mention Award**

Fingerprinting Web Users through Font Metrics
Fifield, D., and Egelman, S. Proceedings of the 19th international conference on Financial Cryptography and Data Security *(FC'15), 2015.*

Somebody's Watching Me? Assessing the Effectiveness of Webcam Indicator Lights
Portnoff, R., Lee, L., Egelman, S., Mishra, P., Leung, D., and Wagner, D. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '15), 2015, New York, NY, USA.*

Are You Ready to Lock? Understanding User Motivations for Smartphone Locking Behaviors
Egelman, S., Jain, S., Portnoff, R. S., Liao, K., Consolvo, S., and Wagner, D. Proc. of the ACM SIGSAC Conference on Computer & Communications Security *(CCS '14), 2014, New York, NY, USA.*

The Effect of Developer-Specified Explanations for Permission Requests on Smartphone User Behavior
Tan, J., Nguyen, K., Theodorides, M., Negron-Arroyo, H., Thompson, C., Egelman, S., and Wagner, D. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '14), 2014, Toronto, Canada.*

The Importance of Being Earnest [in Security Warnings]
Egelman, S., and Schechter, S. Proceedings of the 17th international conference on Financial Cryptography and Data Security *(FC'13), 2013, Okinawa, Japan.*

My Profile Is My Password, Verify Me! The Privacy/Convenience Tradeoff of Facebook Connect
Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '13), 2013, Paris, France.*

Does My Password Go up to Eleven? The Impact of Password Meters on Password Selection
Egelman, S., Sotirakopoulos, A., Muslukhov, I., Beznosov, K., and Herley, C. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '13), 2013, Paris, France.*

When It's Better to Ask Forgiveness than Get Permission: Attribution Mechanisms for Smartphone Resources
Thompson, C., Johnson, M., Egelman, S., Wagner, D., and King, J. Proceedings of the Ninth Symposium on Usable Privacy and Security *(SOUPS '13), 2013, Newcastle, United Kingdom.*

Android permissions: user attention, comprehension, and behavior
Felt, A. P., Ha, E., Egelman, S., Haney, A., Chin, E., and Wagner, D. Proceedings of the Eighth Symposium on Usable Privacy and Security *(SOUPS '12), 2012, Washington, D.C.* **SOUPS Best Paper Award (2012) / SOUPS Impact Award (2017)**

Facebook and privacy: it's complicated
Johnson, M., Egelman, S., and Bellovin, S. M. Proceedings of the Eighth Symposium on Usable Privacy and Security *(SOUPS '12), 2012, Washington, D.C.*

It's all about the Benjamins: Incentivizing users to ignore security advice
Christin, N., Egelman, S., Vidas, T., and Grossklags, J. Proceedings of the 15th international conference on Financial Cryptography and Data Security *(FC'11), 2011, Gros Islet, St. Lucia.*

Oops, I did it again: mitigating repeated access control errors on facebook
Egelman, S., Oates, A., and Krishnamurthi, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '11), 2011, Vancouver, BC, Canada.*

Of passwords and people: measuring the effect of password-composition policies
Komanduri, S., Shay, R., Kelley, P. G., Mazurek, M. L., Bauer, L., Christin, N., Cranor, L. F., and Egelman, S. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '11), 2011, Vancouver, BC, Canada.* **SIGCHI Honorable Mention Award**

Timing is everything?: the effects of timing and placement of online privacy indicators
Egelman, S., Tsai, J., Cranor, L. F., and Acquisti, A. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '09), 2009, Boston, MA, USA.*

It's No Secret: Measuring the Security and Reliability of Authentication via 'Secret' Questions
Schechter, S., Brush, A. J. B., and Egelman, S. Proceedings of the 2009 IEEE Symposium on Security and Privacy *(Oakland '09), 2009, Los Alamitos, CA, USA.*

It's not what you know, but who you know: a social approach to last-resort authentication

Schechter, S., Egelman, S., and Reeder, R. W. Proceedings of the SIGCHI Conference on Human Factors in Computing Systems *(CHI '09), 2009, Boston, MA, USA.*

Crying wolf: an empirical study of SSL warning effectiveness
Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N., and Cranor, L. F. Proceedings of the 18th USENIX Security Symposium *(SSYM'09), 2009, Montreal, Canada.*

Family accounts: a new paradigm for user accounts within the home environment
Egelman, S., Brush, A. J. B., and Inkpen, K. M. Proceedings of the 2008 ACM Conference on Computer Supported Cooperative Work *(CSCW '08), 2008, San Diego, CA, USA.*

You've Been Warned: An empirical study of the effectiveness of browser phishing warnings
Egelman, S., Cranor, L. F., and Hong, J. CHI '08: Proceeding of The 26th SIGCHI Conference on Human Factors in Computing Systems *(CHI '08), 2008, Florence, Italy.* **SIGCHI Honorable Mention Award**

Phinding Phish: Evaluating Anti-Phishing Tools
Zhang, Y., Egelman, S., Cranor, L. F., and Hong, J. Proceedings of the 14th Annual Network & Distributed System Security Symposium *(NDSS '07), 2007, San Diego, CA.*

Power Strips, Prophylactics, and Privacy, Oh My!
Gideon, J., Egelman, S., Cranor, L., and Acquisti, A. Proceedings of the Second Symposium on Usable Privacy and Security *(SOUPS '06), 2006, Pittsburgh, PA.*

An analysis of P3P-enabled web sites among top-20 search results
Egelman, S., Cranor, L. F., and Chowdhury, A. Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet *(ICEC '06), 2006, Fredericton, New Brunswick, Canada.*

refereed workshop publications

Identifying and Classifying Third-Party Entities in Natural Language Privacy Policies
Hosseini, M. B., Pragyan, K., Reyes, I., and Egelman, S. Proceedings of the Second Workshop on Privacy in Natural Language Processing *(PrivateNLP '20), 2020.*

Do You Get What You Pay For? Comparing The Privacy Behaviors of Free vs. Paid Apps
Han, C., Reyes, I., On, A. E. B., Reardon, J., Feal, A., Bamberger, K. A., Egelman, S., and Vallina-Rodriguez, N. The Workshop on Technology and Consumer Protection *(ConPro '19), 2019.*

Privacy Controls for Always-Listening Devices
Malkin, N., Egelman, S., and Wagner, D. Proceedings of the New Security Paradigms Workshop *(NSPW '19), 2019, San Carlos, Costa Rica.*

On The Ridiculousness of Notice and Conset: Contradictions in App Privacy Policies
Okoyomon, E., Samarin, N., Wijesekera, P., On, A. E. B., Vallina-Rodriguez, N., Reyes, I., Feal, A., and Egelman, S. The Workshop on Technology and Consumer Protection *(ConPro '19), 2019.*

Better Late(r) than Never: Increasing Cyber-Security Compliance by Reducing Present Bias
Frik, A., Egelman, S., Harbach, M., Malkin, N., and Peer, E. Workshop on the Economics of Information Security *(WEIS '18), 2018.*

"What Can't Data Be Used For?" Privacy Expectations about Smart TVs in the U.S.
Malkin, N., Bernd, J., Johnson, M., and Egelman, S. Proceedings of the European Workshop on Usable Security *(EuroUSEC '18), 2018.*

Personalized Security Messaging: Nudges for Compliance with Browser Warnings
Malkin, N., Mathur, A., Harbach, M., and Egelman, S. Proceedings of the European Workshop on Usable Security *(EuroUSEC '17), 2017.*

"Is Our Children's Apps Learning?" Automatically Detecting COPPA Violations
Reyes, I., Wijesekera, P., Razaghpanah, A., Reardon, J., Vallina-Rodriguez, N., Egelman, S., and Kreibich, C. The Workshop on Technology and Consumer Protection *(ConPro '17), 2017.*

Information Disclosure Concerns in The Age of Wearable Computing
Lee, L. N., Lee, J. H., Egelman, S., and Wagner, D. Proceedings of the NDSS Workshop on Usable Security *(USEC '16), 2016.*

The Myth of the Average User:
Improving Privacy and Security Systems through Individualization
Egelman, S., and Peer, E. Proceedings of the 2015 Workshop on New Security Paradigms *(NSPW '15), 2015, Twente, The Netherlands.*

Teaching Privacy: What Every Student Needs to Know
Friedland, G., Egelman, S., and Garcia, D. Proceedings of the 46th SIGCSE technical symposium on computer science education *(Workshop), 2015.*

U-PriSM 2: The Second Usable Privacy and Security for Mobile Devices Workshop
Chiasson, S., Crawford, H., Egelman, S., and Irani, P. Proc. of the 15th International Conference on Human-computer Interaction with Mobile Devices and Services *(MobileHCI '13), 2013, Munich, Germany.*

Markets for Zero-day Exploits: Ethics and Implications
Egelman, S., Herley, C., and Oorschot, P. C. van Proceedings of the 2013 Workshop on New Security Paradigms Workshop *(NSPW '13), 2013, Banff, Alberta, Canada.*

Choice Architecture and Smartphone Privacy: There's A Price for That
Egelman, S., Felt, A. P., and Wagner, D. The 2012 Workshop on the Economics of Information Security *(WEIS '12), 2012, Berlin, Germany.*

How Good Is Good Enough? The sisyphean struggle for optimal privacy settings
Egelman, S., and Johnson, M. Proceedings of the Reconciling Privacy with Social Media Workshop *(CSCW '12 Workshop), 2012, Seattle, WA.*

It's Not Stealing if You Need It: A Panel on the Ethics of Performing Research Using Public Data of Illicit Origin
Egelman, S., Bonneau, J., Chiasson, S., Dittrich, D., and Schechter, S. Proceedings of the 16th International Conference on Financial Cryptography and Data Security *(FC'12), 2012.*

How to ask for permission
Felt, A. P., Egelman, S., Finifter, M., Akhawe, D., and Wagner, D. Proceedings of the 7th USENIX conference on Hot Topics in Security *(HotSec'12), 2012, Bellevue, WA.*

I've got 99 problems, but vibration ain't one: a survey of smartphone users' concerns
Felt, A. P., Egelman, S., and Wagner, D. Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices *(SPSM '12), 2012, Raleigh, North Carolina, USA.*

Toward Privacy Standards Based on Empirical Studies
Egelman, S., and McCallister, E. The Workshop on Web Tracking and User Privacy *(W3C Workshop), 2011, Princeton, NJ.*

Please Continue to Hold: An Empirical Study on User Tolerance of Security Delays
Egelman, S., Molnar, D., Christin, N., Acquisti, A., Herley, C., and Krishnamurthi, S. Workshop on the Economics of Information Security (WEIS '10) *(WEIS '10), 2010, Cambridge, MA.*

Tell Me Lies: A Methodology for Scientifically Rigorous Security User Studies
Egelman, S., Tsai, J., and Cranor, L. F. Proceedings of the Workshop on Studying Online Behavior *(CHI '10 Workshop), 2010, Atlanta, GA.*

This is Your Data on Drugs: Lessons Computer Security Can Learn from the Drug War
Molnar, D., Egelman, S., and Christin, N. Proceedings of the 2010 Workshop on New Security Paradigms *(NSPW '10), 2010, Concord, Massachusetts, USA.*

Security user studies: methodologies and best practices
Egelman, S., King, J., Miller, R. C., Ragouzis, N., and Shehan, E. CHI '07 Extended Abstracts on Human Factors in Computing Systems *(CHI EA '07), 2007, San Jose, CA, USA.*

The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study
Tsai, J., Egelman, S., Cranor, L., and Acquisti, A. Proceedings of the 2007 Workshop on the Economics of Information Security *(WEIS '07), 2007, Pittsburgh, PA, USA.*

Studying the Impact of Privacy Information on Online Purchase Decisions
Egelman, S., Tsai, J., Cranor, L. F., and Acquisti, A. Proceedings of the Workshop on Privacy and HCI: Methodologies for Studying Privacy Issues *(CHI '06 Workshop), 2006, Montreal, Canada.*

book chapters and magazine articles

50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System
Reardon, J., Feal, Á., Wijesekera, P., On, A. E. B., Vallina-Rodriguez, N., and Egelman, S. *;login:* 2019, USENIX Association.

Predicting Privacy and Security Attitudes
Egelman, S., and Peer, E. *Computers and Society*, 2015, ACM.

Crowdsourcing
Egelman, S., Chi, E., and Dow, S. *Ways of Knowing in HCI*, 2013, Springer.

Helping users create better passwords
Ur, B., Kelley, P. G., Komanduri, S., Lee, J., Maass, M., Mazurek, M., Passaro, T., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L. F., Egelman, S., and Lopez, J. *;login:* 2012, USENIX Association.

Suing Spammers for Fun and Profit
Egelman, S. *;login:* 2004, USENIX Association.

Installation
Egelman, S. *Peter Norton's Complete Guide to Linux*, 1999, Macmillan Computer Publishing.

User Administration
Egelman, S. *Peter Norton's Complete Guide to Linux*, 1999, Macmillan Computer Publishing.

awards and recognition

2022 **Emilio Aced Personal Data Protection Research Award**
50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System, with J. Reardon, A. Feal, P. Wijesekera, A. Elazari Bar On, and N. Vallina-Rodriguez.

2020 **Caspar Bowden Award for Outstanding Research in Privacy Enhancing Technologies**
"Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale, with I. Reyes, P. Wijesekera, J. Reardon, A. Elazari, A. Razaghpanah, and N. Vallina-Rodriguez.

2019 **USENIX Security Symposium Distinguished Paper Award**
50 Ways to Leak Your Data: An Exploration of Apps' Circumvention of the Android Permissions System, with J. Reardon, A. Feal, P. Wijesekera, A. Elazari Bar On, and N. Vallina-Rodriguez.

2018 **SIGCHI Honorable Mention Award (Best Paper Nominee)**
Contextualizing Privacy Decisions for Better Prediction (and Protection), with P. Wijesekera, J. Reardon, I. Reyes, L. Tsai, J.-W. Chen, N. Good, D. Wagner, and K. Beznosov.

2017 **Symposium on Usable Privacy and Security (SOUPS) Impact Award**
Android Permissions: User Attention, Comprehension, and Behavior, with A. P. Felt, E. Ha, A. Haney, E. Chin, and D. Wagner.

Senior Member Association for Computing Machinery (ACM)

2016 **Symposium on Usable Privacy and Security (SOUPS) Distinguished Poster Award**
Risk Compensation in Home-User Computer Security Behavior: A Mixed-Methods Exploratory Study, with S. Pearman, A. Kumar, N. Munson, C. Sharma, L. Slyper, L. Bauer, and N. Christin.

SIGCHI Honorable Mention Award (Best Paper Nominee)
Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS), with M. Harbach and E. Peer.

SIGCHI Honorable Mention Award (Best Paper Nominee)
The Anatomy of Smartphone Unlocking: A Field Study of Android Lock Screens, with M. Harbach and A. De Luca.

SIGCHI Honorable Mention Award (Best Paper Nominee)
Keep on Lockin' in the Free World: A Transnational Comparison of Smartphone Locking, with M. Harbach, A. De Luca, and N. Malkin.

2015 **SIGCHI Honorable Mention Award (Best Paper Nominee)**
Scaling the Security Wall: Developing a Security Behavior Intentions Scale, with E. Peer.

2012 **AIS Best Publication of 2011**
The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, with J. Tsai, L. Cranor, and A. Acquisti.

ISR Best Published Paper
The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study, with J. Tsai, L. Cranor, and A. Acquisti.

SOUPS Best Paper Award
Android Permissions: User Attention, Comprehension, and Behavior, with A. P. Felt, E. Ha, A. Haney, E. Chin, and D. Wagner.

2011 **SIGCHI Honorable Mention Award (Best Paper Nominee)**
Of Passwords and People: Measuring the Effect of Password-Composition Policies, with S. Komanduri, R. Shay, P. G. Kelley, M. Mazurek, L. Bauer, N. Christin, and L. F. Cranor.

2008 **SIGCHI Honorable Mention Award (Best Paper Nominee)**
You've Been Warned: An Empirical Study on the Effectiveness of Web Browser Phishing Warnings, with L. Cranor and J. Hong.

2006 **Tor Graphical User Interface Design Competition**
Phase 1 Overall Winner, with L. Cranor, J. Hong, P. Kumaraguru, C. Kuo, S. Romanosky, J. Tsai, and K. Vaniea.

Publisher's Clearing House Finalist
I *may* already be a winner.

expert testimony and reports

2022 Expert witness for the District of Columbia Office of the Attorney General in *District of Columbia v. Town Sports International LLC*. I provided a rebuttal report on proper surveying methodology and was deposed by opposing counsel.

2021 Expert witness testifying before the U.S. Senate (Committee on Commerce, Science, and Transportation), hearing on "Protecting Kids Online: Internet Privacy and Manipulative Marketing." Testimony available at: https://www.commerce.senate.gov/2021/5/protecting-kids-online-internet-privacy-and-manipulative-marketing

2019-2020 Expert witness for the plaintiffs in *The People of the State of California v. TWC Product and Technology, LLC, LASC No. 19STCV00605*, providing technical privacy analysis of mobile apps and assisting with discovery strategy in a case stemming from the alleged inappropriate collection of location data from The Weather Channel app.

2017-2019 Expert witness for the plaintiffs in *Vizio, Inc., Consumer Privacy Litigation, No. 8:16-ml-02693-JLS-KES*, assisting with discovery strategy and providing explanations of relevant privacy research on users' willingness to pay for privacy in order to assist in quantifying damages.

2016 Expert witness for the FTC in *Federal Trade Commission vs. Amazon.com, Inc., No. C14-1038-JCC*, providing testimony on human-computer interaction (HCI) evaluation methods and critiquing opposing expert's report.

2014-2015 Expert witness for the plaintiffs in *Doe vs. Twitter, Inc., No. CGC-10-503630*, providing explanations of relevant privacy research on users' willingness to pay for privacy in order to assist in quantifying damages.

2014 Expert witness for the plaintiffs in *13-cv-22122-Martinez/Goodman (S.D. Florida)*, providing written testimony on basic human-computer interaction concepts as they relate to smartphone usage.

2013 Expert witness for the plaintiffs in *LinkedIn User Privacy Litigation, No. 12-cv-03088-EJD (N.D. Cal.)*, providing explanations of information security concepts and providing original research on users' privacy expectations in order to demonstrate and quantify damages.

2012 Expert witness for the plaintiffs in *Netflix Privacy Litigation, No. 5:11-cv-00379-EJD (N.D. Cal.)*, providing explanations of relevant privacy research and the economics of information privacy in order to quantify damages.

grants awarded

2019 **Google: ASPIRE: SDK Traffic Identification at Scale** $75,000
Principal Investigator

2018-2022 **NSF: Mobile Dynamic Privacy and Security Analysis at Scale (CNS-1817248)** $668,475
Principal Investigator

2018-2022 **NSF: Contextual Integrity: From Theory to Practice (CNS-1801501/1801307/1801316)**
$1,199,462
Principal Investigator (Collaborative with Helen Nissenbaum, Cornell University; and Norman Sadeh, Carnegie Mellon University)

2018-2021 **NSF: Increasing Users' Cyber-Security Compliance by Reducing Present Bias (CNS-1817249)** $558,018
Principal Investigator

2018-2023 **NSA: The Science of Privacy:**
Implications for Data Usage (H98230-18-D-0006) $3,236,424
Principal Investigator (Co-PI: Michael Tschantz, International Computer Science Institute)

2018-2019 **DHS: Scaling Contextual Privacy to MDM Environments (FA8750-18-2-0096)** $480,000
Principal Investigator

2018-2019 **Rose Foundation: AppCensus: Mobile App Privacy Analysis at Scale** $40,000
Principal Investigator (Co-PI: Irwin Reyes, International Computer Science Institute)

2018 **Cisco: Access Controls for an IoT World** $99,304
Principal Investigator

2018 **CLTC: Privacy Analysis at Scale** $50,000
Principal Investigator

2018 **CLTC: Secure Internet of Things for Senior Users** $60,590
Co-PI (PI: Alisa Frik, International Computer Science Institute)

2017 **Mozilla: Towards Usable IoT Access Controls in the Home** $46,000
Principal Investigator

2017 **Data Transparency Lab (DTL) / AT&T: Transparency via Automated Dynamic Analysis at Scale** $55,865
Principal Investigator

2017 **CLTC: Secure & Usable Backup Authentication** $48,400
Co-PI (PI: David Wagner, University of California, Berkeley)

2016 - 2017 **NSF: Teaching Security in CSP (CNS-1636590)** $200,000
Co-PI (PI: Julia Bernd, ICSI)

2016 - 2017 **DHS: A Platform for Contextual Mobile Privacy (FA8750-16-C-0140)** $664,378
Principal Investigator

2016 - 2018 **CLTC: The Security Behavior Observatory** $195,962
Principal Investigator

2016 **CLTC: Using Individual Differences to Tailor Security Mitigations** $100,000
Principal Investigator

2015 - 2018 **NSF/BSF: Using Individual Differences to Personalize Security Mitigations (CNS-1528070/BSF-2014626)** $724,732
Principal Investigator (Collaborative with Eyal Peer, Bar-Ilan University)

2015 - 2019 **NSF: Security and Privacy for Wearable and Continuous Sensing Platforms (CNS-1514211/1514457/1513584)** $1,200,000
Principal Investigator (Collaborative with David Wagner, University of California, Berkeley; and Franziska Roesner, University of Washington)

2014 - 2016 **NSF: Teachers' Resources for Online Privacy Education (DGE-1419319)** $300,000
Co-PI (PI: Gerald Friedland, ICSI)

2014 - 2017 **NSA: User Security Behavior** $200,000
Subcontract (PIs: Lorrie Cranor, Rahul Telang, Alessandro Acquisti, and Nicholas Christin; Carnegie Mellon University)

2014 **Google: Improving Security Warnings by Examining User Intent** $71,500
Principal Investigator

2013 - 2015 **NSF: Designing Individualized Privacy and Security Systems (CNS-1343433/1343451)** $132,620
Principal Investigator (Collaborative with Eyal Peer, Carnegie Mellon University)

2013 - 2016 **NSF: A Choice Architecture for Mobile Privacy and Security (CNS-1318680)** $500,000
Co-PI (PI: David Wagner, University of California, Berkeley)

2010 **Google: Designing Usable Certificate Dialogs in Chrome** $60,000
Principal Investigator

professional activities

program committees

2020 ACM CCS; Workshop on Economics and Information Security (WEIS); Symposium on Usable Privacy and Security (SOUPS); USENIX Security

2019 Privacy Enhancing Technologies Symposium (PETS); Workshop on Economics and Information Security (WEIS); Symposium on Usable Privacy and Security (SOUPS)

2018 ACM SIGCHI (Human Factors in Computing Systems); Privacy Enhancing Technologies Symposium (PETS); Workshop on Economics and Information Security (WEIS); ACM Conference on Computer and Communications Security (CCS); Symposium on Usable Privacy and Security (SOUPS); IEEE Security & Privacy ("Oakland")

2017 ACM SIGCHI (Human Factors in Computing Systems); USENIX Security; Privacy Enhancing Technologies Symposium (PETS); New Security Paradigms Workshop (NSPW), **Co-Chair**; Workshop on Economics and Information Security (WEIS); ACM Conference on Computer and Communications Security (CCS); Symposium on Usable Privacy and Security (SOUPS)

2016 Workshop on the Economics of Information Security (WEIS), **Chair**; New Security Paradigms Workshop (NSPW), **Co-Chair**; ACM SIGCHI (Human Factors in Computing Systems); USENIX Security; Symposium on Usable Privacy and Security (SOUPS); ACM WWW; Financial Cryptography and Data Security; Privacy Enhancing Technologies Symposium (PETS)

2015	Symposium on Usable Privacy and Security (SOUPS); USENIX Security; ACM SIGCHI (Human Factors in Computing Systems); Privacy Enhancing Technologies Symposium (PETS); Workshop on the Economics of Information Security (WEIS); ACM WWW; Financial Cryptography and Data Security
2014	ACM SIGCHI (Human Factors in Computing Systems); Financial Cryptography and Data Security; ACM WWW; Privacy Enhancing Technologies Symposium (PETS)
2013	ACM SIGCHI (Human Factors in Computing Systems); Symposium on Usable Privacy and Security (SOUPS); New Security Paradigms Workshop (NSPW); Anti-Phishing Working Group eCrime Researchers Summit
2012	Symposium on Usable Privacy and Security (SOUPS); New Security Paradigms Workshop (NSPW)
2011	Symposium On Usable Privacy and Security (SOUPS); New Security Paradigms Workshop (NSPW); Computers, Freedom, and Privacy (CFP) Conference (poster session co-chair); Software and Usable Security Aligned for Good Engineering (SAUSAGE) Workshop, **Co-Chair**
2010	Symposium On Usable Privacy and Security (SOUPS)
2008	Conference on Information and Knowledge Management (CIKM)
2007	ACM SIGCHI Workshop - Security User Studies: Methodologies and Best Practices; Anti-Phishing Working Group eCrime Researchers Summit (poster session co-chair)
2006	Computers, Freedom, and Privacy (CFP) Conference

standards committees

2007-2008	W3C Web Security Context (WSC) Working Group
2004-2006	W3C Platform for Privacy Preferences (P3P) 1.1 Working Group

leadership roles

2021-Now	Member, ICSI Scientific Leadership Council
2012-Now	Director, Berkeley Laboratory for Usable and Experimental Security (BLUES)
2006-2008	Legislative Concerns Chair / Board of Directors, National Association of Graduate and Professional Students (NAGPS)
2006-2008	Vice President for External Affairs, Carnegie Mellon Graduate Student Assembly

teaching

Fall 2019 **Usable Privacy and Security** University of California, Berkeley
Designed and taught a course as part of the School of Information's Masters in Cybersecurity program. Duties included course design and development, grading assignment and exams, supervising class projects, and holding office hours.

Spring 2017, Spring 2018 **Human Factors in Computer Security and Privacy** Brown University
Instructor for a module on "user interfaces for security" as part of the Executive Masters in Cybersecurity program. Duties included course design and development, grading assignments and exams, supervising thesis projects, and holding office hours.

Fall 2007 **Information Security & Privacy (46-861)** Carnegie Mellon University
Teaching assistant duties included developing course materials (topics for lectures, assignments, and exams), grading assignments and exams, holding office hours, and mentoring students about semester-long projects.

Spring 2006	**Computers and Society (15-290)**	Carnegie Mellon University
	Teaching assistant duties included giving guest lectures, creating assignments and exams, grading assignments and exams, holding office hours, and mentoring students about semester-long projects.	
Fall 2003	**Information Security (CS 451)**	University of Virginia
	Teaching assistant duties included giving guest lectures, creating assignments and exams, grading assignments and exams, and holding office hours.	
Fall 2003	**Intellectual Property (TCC 200)**	University of Virginia
	Teaching assistant duties included grading assignments and holding office hours.	
Spring 2003, Spring 2004	**Advanced Software Development Methods (CS 340)**	University of Virginia
	Teaching assistant duties included grading and holding office hours.	
Fall 2002	**Engineering Software (CS 201J)**	University of Virginia
	Teaching assistant duties included grading assignments and holding office hours.	